Discrete Applied Mathematics 157 (2009) 3320–3326

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Note

APN permutations on $\mathbb{Z}_n$ and Costas arrays

Konstantinos Drakakis [a,c], Rod Gow [b,c], Gary McGuire [b,c,*]

[a] School of Electrical, Electronic, and Mechanical Engineering, University College Dublin, Belfield, Dublin 4, Ireland
[b] School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland
[c] UCD CASL, University College Dublin, Belfield, Dublin 4, Ireland

ARTICLE INFO

Article history:
Received 13 June 2008
Received in revised form 9 May 2009
Accepted 22 June 2009
Available online 8 July 2009

Keywords:
Almost Perfect Nonlinear (APN) permutations
Welch–Costas permutations

ABSTRACT

We study PN and APN functions over the integers modulo n. We give some construction techniques based on Costas arrays, which allow us to construct APN permutations on $\mathbb{Z}_{p-1}$ where p is a prime. Although PN permutations do not exist, one set of our functions is very close to being a set of PN permutations.

1. Introduction

Perfect Nonlinear (PN) and Almost Perfect Nonlinear (APN) functions find many applications in cryptography and coding theory. Due to the binary operation principle of modern computers, increasing emphasis has been placed on APN functions defined from the additive group of a finite field of characteristic 2 to itself. The group in question here is an elementary abelian 2-group. However, PN and APN functions can be defined between any two abelian groups. One Soviet version of the Data Encryption Standard, known as GOST, uses a function from a cyclic group to an elementary abelian group, both of order 16 (see [5]). In this paper we will consider functions from a cyclic group to itself.

There are certain advantages in having an APN function which is also a permutation (it is easy to see that PN permutations do not exist, see Section 2.2). The basic properties of APN permutations on $(\mathbb{Z}_2)^n$ were outlined in [1]. One of the big open problems in the area of APN functions is the existence of an APN permutation on a finite field of order 2^n where n is even. Computer searches have shown that none exists for $n = 4$. In this work, we focus on APN functions defined on $\mathbb{Z}_n$, the ring of integers modulo n. Permutation polynomials on $\mathbb{Z}_n$ have been studied by Mullen and Stevens in [4], and have been studied for cryptographic applications by Rivest in [6]. The SAFER family of cryptosystems, proposed by Massey [3] uses APN functions from $\mathbb{Z}_{256}$ to itself. In this context, the definition of PN/APN functions is very similar to the definition of a type of permutation known as a Costas permutation, and this similarity motivated the present paper. We will look into the possibility of using Costas permutation construction techniques to construct new families of APN permutations. We show that one construction of Costas permutations, known as the Welch construction, gives APN permutations on $\mathbb{Z}_{p-1}$, where p is a prime. The maps are almost PN, in a sense we will make precise.

After reviewing the relevant definitions in Section 2, we shall review some Costas permutation constructions in Section 3, and show that stronger properties actually hold. In Section 4 we will prove that the Welch construction method for Costas permutations can indeed be used to construct APN permutations. We will also see that the APN permutations so constructed are "almost" PN permutations, requiring just a small relaxation of the definition. Section 5 is a short section on applications

* Corresponding author at: School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland. Fax: +353 17165236.
E-mail addresses: Konstantinos.Drakakis@ucd.ie (K. Drakakis), Rod.Gow@ucd.ie (R. Gow), Gary.McGuire@ucd.ie (G. McGuire).

0166-218X/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2009.06.029

to cryptography. We will offer complete enumeration results in Section 6 for APN permutations for $n \leq 18$, and determine how many of those are also Costas arrays.

2. Definitions and easy results

We will use extensively the shorthand notation $[n] := \{0, \ldots, n-1\}$ for $n \in \mathbb{N}$, while p will consistently denote a prime number. As in the next sections we are going to have arithmetic modulo p and $p-1$ combined together in some sense, we will outline the general principle of what we will do here, to avoid confusion later.

For any given permutation $\sigma : [n] \to [n]$, we can define a function $\hat{\sigma}$ from $\mathbb{Z}_n \to \mathbb{Z}_n$. In fact, we could use σ to define a function between any two groups of order n, but there is a natural way of doing so for $\mathbb{Z}_n$. The function is thus defined in the natural way, by $\hat{\sigma}(\bar{j}) := \overline{\sigma(j)}$, where $\bar{r}$ denotes the residue class of r in $\mathbb{Z}_n$, and $j, \sigma(j)$ are the representatives of the classes $\bar{j}, \overline{\sigma(j)}$ that lie between 0 and $n-1$.

In the next sections we will carry out this construction in the case $n = p-1$, where p is a prime. The initial permutation (which we will denote by f) will be constructed using arithmetic modulo p, but will be a permutation of $[p-1]$. We will then forget about the origins of the permutation f and carry out the construction of the previous paragraph to obtain a permutation of $\mathbb{Z}_{p-1}$.

2.1. (Almost) Perfect Nonlinearity and Costas permutations

The definitions of a Costas permutation and an APN permutation are very close. We begin by offering the relevant definitions.

Definition 1 (*Costas Permutation*). A permutation $f : [n] \to [n]$ is Costas iff

$$\forall i, j, k \in [n] : i + k, j + k \in [n], \quad f(i+k) - f(i) = f(j+k) - f(j) \Longrightarrow k = 0 \quad \text{or} \quad i = j.$$

Furthermore, f is domain-periodic Costas (D-periodic Costas for short) modulo N iff

$$\forall i, j, k \in [n], \quad f((i+k) \bmod N) - f(i) = f((j+k) \bmod N) - f(j) \Longrightarrow k = 0 \quad \text{or} \quad i = j,$$

and f is range-periodic Costas (R-periodic Costas for short) modulo N iff

$$\forall i, j, k \in [n] : i + k, j + k \in [n], \quad (f(i+k) - f(i)) \bmod N = (f(j+k) - f(j)) \bmod N \Longrightarrow k = 0 \quad \text{or} \quad i = j.$$

The latter two properties are stronger and imply the Costas property. When $N = n$, f will simply be called D-/R-periodic. A D-periodic Costas permutation can be construed to be defined on $\mathbb{Z}_n$, while an R-periodic Costas permutation to take values in $\mathbb{Z}_n$. The two properties can be combined to yield domain-and-range-periodic (DR-periodic) Costas permutations.

Definition 2 (*Perfect Nonlinear Function*). Let G_1, G_2 be finite abelian groups, written additively, of the same cardinality. We say $f : G_1 \to G_2$ is a Perfect Nonlinear (PN) function iff $f(x+a) - f(x) = b$ has exactly one solution for all $a \in G_1$, $a \neq 0$, and all $b \in G_2$. Equivalently, $f(x+a) - f(x) = f(y+a) - f(y) \Longrightarrow a = 0$ or $x = y$.

PN functions do not exist on fields of characteristic 2, because if x is a solution to $f(x+a) - f(x) = b$ then so is $x + a$. This is why the following definition is made.

Definition 3 (*Almost Perfect Nonlinear Function*). Let G_1, G_2 be finite abelian groups, written additively, of the same cardinality. We say $f : G_1 \to G_2$ is an Almost Perfect Nonlinear (APN) function iff $f(x+a) - f(x) = b$ has at most two solutions for all $a \in G_1$, $a \neq 0$ and all $b \in G_2$.

Remark 1. Definitions 1 and 2 are deceptively close, but there are three important differences:

1. PN/APN functions are not required to be permutations, and, as a matter of fact, they rarely are.
2. Costas permutations are defined on integers $[n]$, whereas PN/APN functions are defined more generally on any abelian group.
3. Addition appearing in the definition of a Costas permutation is the usual integer addition in $\mathbb{Z}$, which means that $i + k$ or $j + k$ could fall outside the domain of definition of the function. This does not happen for a PN/APN function.

Remark 2. Consider the square array corresponding to a bijection f (according, for example, to the convention that $f(x) = y$ implies that the element (y, x) of the array A_f is 1, while all other elements in column x are 0). Consider further that 1s are represented by dots, 0s by blanks, and consider all possible linear segments between pairs of dots.

- The Costas property is equivalent to the fact that no two linear segments have both the same length and slope. The array is known as a Costas array in the literature [2].
- The PN property implies that the Costas property still holds even when the array is wrapped on a torus.
- The APN property implies that three or more linear segments cannot have the same length and slope, when the array is wrapped on a torus.

2.2. Simple consequences

The following are simple consequences of the definitions in the previous section:

Theorem 1. *PN permutations do not exist.*

Proof. Let f be a PN function. Choosing b in Definition 2 to be 0, for all nonzero a there must exist a solution to $f(x+a) - f(x) = 0$. Therefore, f cannot be a permutation. □

Remark 3. The classic example of a PN function on a finite field of odd characteristic is $f(x) = x^2$: f is clearly not bijective since $f(1) = f(-1)$, but it is PN since $f(x+a) - f(x) = 2ax + a^2 = b$ for $a \neq 0$ has exactly one root x, because $2a$ is invertible. On a general ring $\mathbb{Z}_n$, however, f is no longer PN, as the number of roots equals either $\gcd(2a, n)$ or 0, depending on b. The closest we can come is when $n = 2p$, p prime, where $\gcd(2a, n) = 2$ for all $a \in \mathbb{Z}_n \setminus \{0, p\}$.

Theorem 2. *The inverse of an APN bijection is also an APN bijection.*

Proof. Definition 3 implies that, for every pair (a, b), at most two vectors with these two coordinates exist in the corresponding permutation array; the result for APN follows from the facts that (a) the inverse permutation corresponds to the transposed permutation array, and (b) that vector populations are not affected by transposition. □

2.3. The difference triangle of a permutation

A very useful tool for detecting the Costas property in a permutation is the difference triangle (DT) T (or $T(f)$ if we need to emphasize the permutation whose DT we consider):

Definition 4. Let $f : [n] \to [n]$ be a function; its Difference Triangle (DT) $T(f)$ is the collection of vectors $T_k,\ k = 1, \ldots, n-1$ (called the rows of the DT), where $T_k = (t_{k1}, \ldots, t_{k,n-k})$, $t_{ki} = f(i+k) - f(i)$, and its Difference Square (DS) $S(f)$ is the collection of vectors $S_k,\ k = 1, \ldots, \left\lceil \frac{n-1}{2} \right\rceil$ (called the rows of the DS), where $S_k = (s_{k1}, \ldots, s_{k,n})$, $t_{ki} = f((i+k) \bmod n) - f(i)$.

A comparison with Definition 1 shows immediately that f is Costas/D-periodic Costas iff no row of the DT/ST has a repeated entry; if this property holds for the values of the DT/ST modulo n, f is R-periodic Costas as well.

3. Construction methods for Costas permutations

There are two algebraic constructions for Costas permutations, based on finite fields, known as the Welch and Golomb constructions [2]. The former is of interest to us, as it yields APN permutations. For the rest of this paper, p will denote an odd prime, and g a primitive element of $\mathbb{Z}_p$ (meaning that the powers of g make up all nonzero elements of $\mathbb{Z}_p$).

3.1. Exponential Welch construction

Definition 5. Let $\mathbb{Z}_p$ be the finite field of prime order p, $p > 2$, let g be a primitive root of $\mathbb{Z}_p$, and let $N_p = \mathbb{Z}_p \setminus \{0\}$, the multiplicative subgroup of $\mathbb{Z}_p$. The *exponential Welch–Costas bijection* $f : \mathbb{Z}_{p-1} \to N_p$ is defined by the formula $f(i) = g^i$.

Note that the domain of f is naturally $\mathbb{Z}_{p-1}$ since $g^{p-1} = 1$.

Theorem 3. *Using the notation of the previous paragraph, f is D-periodic Costas, and R-periodic Costas modulo p.*

Proof. In $\mathbb{Z}_p$,

$$f(i+k) - f(i) = f(j+k) - f(j) \Longrightarrow g^{i+k} - g^i = g^{j+k} - g^j \Longrightarrow g^i(g^k - 1) = g^j(g^k - 1).$$

If $k \neq 0$ then $g^k \neq 1$ so we obtain $g^i = g^j$, which implies $i = j$ (as elements of $\mathbb{Z}_{p-1}$). □

3.2. Logarithmic Welch construction

Definition 6. Let f be an exponential Welch–Costas bijection as defined in Definition 5. The *logarithmic Welch–Costas bijection* $h : N_p \to \mathbb{Z}_{p-1}$ is the inverse of f, defined through the discrete logarithm as $h(i) = \log_g(i)$.

We claim that this function is R-periodic (but not D-periodic) Costas.

Theorem 4. *Using the notation of the previous paragraph,* $\log_g$ *is R-periodic Costas:*

$$\forall i, j, k \in N_p : \ i + k, j + k \in N_p, \qquad \log_g(i + k) - \log_g(i) = \log_g(j + k) - \log_g(j) \Longrightarrow i = j.$$

Proof.

$$\log_g(i + k) - \log_g(i) = \log_g(j + k) - \log_g(j) \Leftrightarrow \log_g\left(\frac{i + k}{i}\right) = \log_g\left(\frac{j + k}{j}\right) \Leftrightarrow \frac{i + k}{i} = \frac{j + k}{j} \Leftrightarrow ik = jk \Leftrightarrow i = j. \quad \square$$

To summarize:

- Exponential Welch–Costas bijections are D-periodic Costas modulo $p - 1$ and R-periodic modulo p;
- Logarithmic Welch–Costas bijections are R-periodic Costas modulo $p - 1$.

3.3. Non-existence results

We now offer some negative results. We have just shown that both exponential and logarithmic Welch–Costas bijections are R-periodic Costas (under the appropriate modulo operator) over a set of *even* size. We now show that this fact is indeed relevant.

Theorem 5. *Let* n *be odd, and let* f *be a Costas permutation on* $[n]$*. Then* f *cannot be R-periodic Costas.*

Proof. Let us consider $T(f)$, the difference triangle of f, and focus on its first row, which contains $n - 1$ entries. By the Costas property, the entries are all different when considered in $\mathbb{Z}$. Assuming that f is R-periodic Costas, all these entries should be distinct modulo n, and hence they should be a permutation of the integers $1, \ldots, n - 1$. The sum of these numbers is $\frac{n(n-1)}{2}$ which is $\equiv 0 \bmod n$ as n is odd. But sum of the entries of the first row of $T(f)$ is

$$f(2) - f(1) + f(3) - f(2) + \cdots + f(n) - f(n + 1) = f(n) - f(1),$$

whence we get that $f(n) - f(1) \equiv 0 \bmod n$. But, given the range of f, the only possibility is $f(1) = f(n)$, which violates our assumption that f is a permutation. This completes the proof. $\square$

4. APN permutations

We show that Welch–Costas bijections are APN.

4.1. Exponential Welch APN permutations

Let f be the exponential Welch–Costas bijection as defined Definition 5 of Section 3.1: in other words, $f : \mathbb{Z}_{p-1} \to N_p$ so that $f(i) = g^i$. We now forget about any algebraic structure, and we consider $\mathbb{Z}_{p-1}$ to be the set $\{0, 1, \ldots, p - 2\}$, and also N_p to be the set $\{1, 2, \ldots, p - 1\}$. In order to get a bijection from $[p - 1]$ to $[p - 1]$, we subtract 1 from the values of f. Next, we carry out the construction described at the beginning of Section 2 to obtain a permutation of $\mathbb{Z}_{p-1}$. Overall, through the conventions we have stipulated and the procedure we followed, we have obtained a new function $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$, where $f(i) = (g^i \bmod p) - 1$; this we will call from now on an *exponential Welch–Costas permutation*.

Theorem 6. *Exponential Welch–Costas permutations are APN permutations on* $\mathbb{Z}_{p-1}$*.*

Proof. Use the same notation as above. We must show that among the entries $f(i + k) - f(i)$ (modulo $p - 1$) in any row of the DS, no number occurs more than twice.

First consider the differences as integers. They all lie between $-(p - 2)$ and $+(p - 2)$. Note that there are $r := (p - 1)/2$ positive differences, and r negative differences, since if $g^{i+k} \bmod p - g^i \bmod p = d$ then $g^{r+i+k} \bmod p - g^{r+i} \bmod p = p - g^{i+k} \bmod p - (p - g^i \bmod p) = -d$, because $g^r = -1 \bmod p$.

Next observe that if we add p to the negative differences, the resulting positive integers are precisely $1, 2, \ldots, p - 1$ in some order. This follows from Theorem 3.

Finally, let the positive differences be $d_1, \ldots, d_r$ and consider adding $p - 1$ to the negative differences (as integers). We obtain the $p - 1$ numbers

$$d_1, d_2, \ldots, d_r, p - 1 - d_1, p - 1 - d_2, \ldots, p - 1 - d_r$$

which are all integers between 1 and $p - 2$. By the pigeonhole principle, some two of these must be equal, and of course several could be equal in principle. We claim that no integer occurs more than twice. For, $d_1, d_2, \ldots, d_r$ are all distinct, and the $p - 1 - d_i$ $(1 \le i \le r)$ are all distinct. And, given d_j, if $p - 1 - d_i = d_j$ then d_i is uniquely determined as $p - 1 - d_j$. $\square$

Consider now an arbitrary Costas permutation $f : [n] \to [n]$, and consider its DS: the pigeonhole principle argument made in the proof above shows that a row of the DS may contain duplicate entries, but it will never contain an entry in triplicate. It follows that, if we keep ordinary integer arithmetic in the range of f, the D-periodic version of f is, in this slight extension of the definition, APN.

Corollary 1. *Any Costas permutation $f : [n] \to [n]$ defines an APN permutation $\tilde{f} : \mathbb{Z}_n \to [n]$, such that $\tilde{f}(i+j) = f((i+j) \bmod n)$.*

4.2. Logarithmic Welch APN permutations

Next we prove the same APN property for logarithmic Welch–Costas bijections. In fact, more can be said in this case. We will see that they are very close to being PN.

Continuing with the conventions of the previous section, a logarithmic Welch–Costas permutation is now defined to be the inverse of the exponential Welch–Costas permutation, namely $\log_g(i+1)$ to make the argument $i+1$ fall in $N_p = \{1, 2, \ldots, p-1\} \subseteq \mathbb{Z}_p$.

Theorem 7. *Logarithmic Welch–Costas permutations $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$ where $f(i) = \log_g(i+1)$ are APN permutations. Furthermore, for each $a \in N$, the function*

$$f_a : \mathbb{Z}_p \setminus \{p-1, p-1-a\} \to \mathbb{Z}_{p-1} \setminus \{0\}, \text{ defined by } f_a(x) := \log_g(x+1+a) - \log_g(x+1)$$

is bijective.

Proof. Since the logarithmic Welch–Costas permutation is the inverse of the exponential, the APN property follows from Theorems 2 and 6. The proof of Theorem 4 proves the second statement. □

It follows that, although PN permutations do not exist by Theorem 1, logarithmic Welch–Costas permutations get as close as possible. They give rise to bijections between subsets of the domain and range of cardinality $p-2$, one bijection for each a. The function f_a, for the various values of a, is not a permutation, because not only are the domain and the range different, but also the domain varies with a.

Remark 4. Another way to view the "almost" PN property is to extend the $\log_g$ function to $\mathbb{Z}_p$ by defining $\infty = \log_g(0)$. Define $\infty + a$ to be ∞ for any $a \in \mathbb{Z}_{p-1}$.

Then Theorem 7 says that for any a, the image of the function $f_a : \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p-1} \cup \{\infty\}$ defined by $f_a(x) = \log_g(x+a) - \log_g(x)$, will consist of ∞ twice and $1, 2, \ldots, p-2$. We will have $f_a(0) = \infty$ and $f_a(p-a) = \infty$. The function f_a is "almost" a bijection. For each a, f_a is a mapping between two finite sets of cardinality p whose image has cardinality $p-1$.

5. Applications

A key component of a Feistel cipher in cryptography is an S-Box. An S-Box can be thought of as a function between two groups. Normally the groups have order 16, 32, 64, 128 or 256. The function in the S-Box is required to have certain properties in order to yield a secure cryptosystem. One of the required properties is the APN property, although this may be slightly compromised in order to improve the overall performance such as in Rijndael (the Advanced Encryption Standard). The APN property ensures resistance to differential cryptanalysis.

Since $p = 17$ is prime, the Welch APN permutations on $\mathbb{Z}_{16}$ are candidates for an S-Box function from $\mathbb{Z}_{16}$ to itself (corresponding to a 4-bit to 4-bit S-Box). The Russian standard GOST uses $\mathbb{Z}_{16}$ already. We are studying these S-Boxes and will present our results in another paper. This gives an S-Box function which is a permutation, whereas no APN permutation exists on a finite field of order 16 as has been checked by computer search.

The SAFER family of cryptosystems, proposed by Massey [3] uses APN functions from $\mathbb{Z}_{256}$ to itself. These are a special case of our construction, where $p = 257$.

6. Enumeration of APN permutations

We present some results on equivalence classes, which help with enumeration. Then we present the results on enumeration of APN permutations on $\mathbb{Z}_n$, and Costas permutations, and the intersection of these two classes, for $n \leq 18$.

Theorem 8. *Let f be an APN function/permutation on $\mathbb{Z}_n$, $n \in \mathbb{N}$; then, $af(c\cdot + d) + b$ where $a, b, c, d \in \mathbb{Z}_n$, $(a, n) = (c, n) = 1$ are also APN functions/permutations. Furthermore, if f is a permutation, the families $\{af + b : a, b \in \mathbb{Z}_n, (b, n) = 1\}$, $\{f(c \cdot + d) : c, d \in \mathbb{Z}_n, (c, n) = 1\}$, $\{af(\cdot + d) : a, d \in \mathbb{Z}_n, (a, n) = 1\}$, and $\{f(c\cdot) + b : b, c \in \mathbb{Z}_n, (c, n) = 1\}$ each consist of distinct permutations.*

Proof. Let us consider the equation:

$$af(c(x+A)+d)+b-[af(cx+d)+b]=B, \quad A\in\mathbb{Z}_n^*,\ B\in\mathbb{Z}_n,$$

which, after simplification, becomes

$$f(y+(Ac+d))-f(y+d)=a^{-1}B, \quad y=cx.$$

Since f is an APN function, there are at most two solutions y for this equation, and as the mapping $x\to y=cx$ is bijective, since c is invertible, the original equation has at most two solutions x. This proves the first statement in the theorem.

Henceforth, let f be a permutation.

- Let a_1f+b_1 and a_2f+b_2 be identical: there exists an x such that $f(x)=0$, hence $b_1=b_2$; similarly, there exists x' such that $f(x')=1$, hence $a_1=a_2$.
- Now let $f(c_1\cdot+d_1)$ and $f(c_2\cdot+d_2)$ be identical: this implies that $c_1\cdot+d_1$ and $c_2\cdot+d_2$ are identical. For any x and y, then, we obtain $c_1x+d_1=c_2x+d_2$ and $c_1y+d_1=c_2y+d_2$, whence $(c_1-c_2)(x-y)=0$. If we now let $x-y=1$, it follows that $c_1=c_2$, whence $d_1=d_2$ too.
- Now let $a_1f(\cdot+d_1)$ and $a_2f(\cdot+d_2)$ be identical: for any x, $a_1f(x+d_1)=a_2f(x+d_2)$. Let $x=x_0$ be the unique value of x such that $f(x_0)=0$; setting $x=x_0-d_1$, we obtain $a_1f(x_0+d_2-d_1)=0$, and, since a_1 is invertible, this implies $f(x_0+d_2-d_1)=0$, which in turn implies that $x_0+d_2-d_1=x_0\Leftrightarrow d_1=d_2$, as f is a permutation. Choosing any x such that $f(x+d_1)$ is invertible, we prove that $a_1=a_2$.
- Now let $f(c_1\cdot)+b_1$ and $f(c_2\cdot)+b_2$ be identical: for any x, $f(c_1x)+b_1=f(c_2x)+b_2$. Letting $x=0$, we obtain $b_1=b_2$. As f is a permutation, it follows that $(c_1-c_2)x=0$, whence, by choosing any invertible x, we prove that $c_1=c_2$.

This completes the proof. □

Corollary 2. *APN permutations of order n can be divided up into disjoint families (equivalence classes) of size divisible by $n[n,\phi(n)]$; if $n=p$ prime, their size becomes divisible by $p^2(p-1)$.*

Proof. Let $T_{a,b}f(x)=af(x)+b$, $S_{c,d}f(x)=f(cx+d)$, and consider the family $\{T_{a,b}S_{c,d}f:\ a,b,c,d\in\mathbb{Z}_n\}$, namely the orbit of f under all possible combinations of T and S operators. Theorem 8 guarantees that the size of this orbit is divisible by both n^2 (considering the subfamily for fixed a and c) and $n\phi(n)$ (considering the subfamily for fixed c and d), hence the size is divisible by $[n^2,n\phi(n)]=n[n,\phi(n)]$. When $n=p$ prime, $\phi(p)=p-1$, which is relatively prime to p, hence $p[p,p-1]=p^2(p-1)$. This completes the proof. □

Enumeration results (see Section 6) actually suggest the following:

Conjecture 1. *Family sizes of APN permutations of order n are divisible by $n^2\phi(n)$.*

The speed of the enumeration of APN permutations can greatly benefit by their grouping into equivalence classes, as explained in Corollary 2. Brute force enumeration requires that each of the $n!$ permutations of order n be tested for the APN property, but efficient code can, in principle, reduce the complexity by a factor of at least $n[n,\phi(n)]$, by considering only one permutation within each equivalence class. In practice, however, it may not be feasible to exploit equivalence completely.

Our code first reduces the complexity by a factor of n, exclusively considering permutations with $f(0)=0$. Consider now the family $T_{a,b}f=af+b$ (in the notation of Corollary 2), and consider the difference

$$D=T_{a,b}f(1)-T_{a,b}f(0)=af(1)-af(0)=af(1)\Leftrightarrow f(1)=a^{-1}D.$$

The code then needs to check $(n-2)!$ permutations times the number of possible values for $f(1)$ that cannot be mapped onto one another through multiplication by units of Z_n. This latter quantity, namely the number of orbits of elements in $\mathbb{Z}_n^*$ whose union spans $\mathbb{Z}_n^*$, is found to be, using the Cauchy–Frobenius Theorem, equal to:

$$\frac{1}{\phi(n)}\sum_{x\in\mathbb{Z}_n^+}(x-1,n)-1,$$

where $\mathbb{Z}_n^+$ denotes the set of units of $\mathbb{Z}^n$. Clearly, the biggest reduction in complexity occurs for $n=p$ prime, where there is only one orbit and the total number of permutations tested is $(p-2)!$.

The complexity can be further reduced through progressive construction of permutations, which allows early termination in case the partial mapping constructed so far already violates the APN property: for example, permutations starting with 1 2 3 4 can be discarded, as the APN property is already violated ($f(x+1)-f(x)=1$ has already got 3 roots).

Enumeration has been carried out for all orders $n\le 18$; the results, along with relevant results for Costas permutations, are presented in Table 1. The following conclusions can be drawn:

- The number of APN permutations of order n is strictly increasing with n (with one exception between 8 and 9), and is much larger than the number of Costas permutations of order n.
- Costas and APN permutations do not overlap significantly. On occasion they may even fail to overlap at all, as is the case for $n=9$; the same phenomenon occurs also for $n=21,23,24,25$.

Table 1
The number of APN permutations on $\mathbb{Z}_n$ for $n \leq 18$. The columns, from left to right, show: the order n; $n!$; the number of APN permutations; the number of APN permutations that are also Costas permutations; the number of Costas permutations of order n.

n	$n!$	|APN|	|APN ∩ C|	|C|
3	6	0	0	4
4	24	16	12	12
5	120	100	40	40
6	720	252	92	116
7	5040	588	112	200
8	40320	2816	140	444
9	362880	1458	0	760
10	3628800	47800	740	2160
11	39916800	136730	448	4368
12	479001600	380736	780	7852
13	6227020800	1614288	668	12828
14	87178291200	4083072	600	17252
15	1307674368000	13305600	300	19612
16	20922789888000	54771712	644	21104
17	355687428096000	147750672	96	18276
18	6402373705728000	560694312	272	15096

7. Conclusion

A first study of APN permutations on $\mathbb{Z}_n$ and of their relation to Costas permutations has been attempted in this paper. We have seen that Welch–Costas permutations are always APN permutations as well, and that logarithmic Welch–Costas permutations, in particular, have further properties that make them "almost" PN permutations, although such an object does not really exist, as we also prove. Otherwise, our enumeration results for APN permutations of order $n \leq 18$ reveal that the relation between APN permutations and Costas arrays is quite erratic.

Acknowledgements

The first author's research was supported by Science Foundation Ireland grants 05/YI2/I677, 06/MI/006, and 08/RFP/MTH1164. The second and third authors' research was supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

References

[1] T. Beth, C. Ding, On almost perfect nonlinear permutations, in: Advances in Cryptology – Eurocrypt' 93, in: Lecture Notes in Computer Science, vol. 765, Springer, New York, 1994, pp. 65–76.
[2] K. Drakakis, A review of costas arrays, Journal of Applied Mathematics (2006).
[3] J.L. Massey, SAFER K-64: A byte-oriented block-ciphering algorithm, Fast Software Encryption, 1993, pp. 1–17.
[4] G. Mullen, H. Stevens, Polynomial functions (mod m), Acta Mathematica, Hungarica 44 (3–4) (1984) 237–241.
[5] A. Pott, Nonlinear functions in abelian groups and relative difference sets, Discrete Applied Mathematics 138 (2004) 177–193.
[6] R. Rivest, Permutation polynomials modulo 2^w, Finite Fields and their Applications 7 (2001) 287–292.